

AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20)

☐ Original ☐ Duplicate Original

LODGED CLERK, U.S. DISTRICT COURT <div style="border: 1px solid black; padding: 5px; text-align: center; font-size: 1.5em;">5/2/2025</div> CENTRAL DISTRICT OF CALIFORNIA BY: _____ MMC _____ DEPUTY
--

UNITED STATES DISTRICT COURT

for the

Central District of California

FILED CLERK, U.S. DISTRICT COURT <div style="border: 1px solid black; padding: 5px; text-align: center; font-size: 1.5em;">5/02/2025</div> CENTRAL DISTRICT OF CALIFORNIA BY: _____ jm _____ DEPUTY

United States of America

v.

Alina Florentina Cocora,

Defendant

Case No. 2:25-MJ-02660-DUTY

**CRIMINAL COMPLAINT BY TELEPHONE
OR OTHER RELIABLE ELECTRONIC MEANS**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of May 1, 2025 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section

18 U.S.C. § 1029(a)(2)

Offense Description

Use of Unauthorized Access Devices

This criminal complaint is based on these facts:

Please see attached affidavit.☒ Continued on the attached sheet.

/s/

Complainant's signature

Alex Le, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 05/02/2025 5:17 pm

Judge's signature

City and state: Los Angeles, California

Hon. Michael Kaufman, U.S. Magistrate Judge

Printed name and title

AUSA: Thi Hoang Ho (x0596)

AFFIDAVIT

I, Alex Le, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against and arrest warrants for Robert Adrian Dinca ("DINCA") and Alina Florentina Cocora ("COCORA") for a violation of 18 U.S.C. §§ 1029(a)(2), (b)(1), (c)(1)(A)(i) (use and attempted use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search a blue iPhone in a black case seized from DINCA (the "SUBJECT DEVICE") and currently in the custody of Homeland Security Investigations, in Paramount, CA, as described in Attachment A.

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1029 (Fraud and Related Activity in Connection with Access Devices), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft) (collectively, the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless

specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent of the United States Department of Health and Human Services ("HHS"), Office of Inspector General ("HHS-OIG"), and I have served in this capacity for approximately three years. I have completed a combined 16 weeks of formal education and training at the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Glynnco, Georgia, and HHS-OIG's Special Agent Basic Training program in Largo, Maryland. This training included instruction in conducting investigations of access device, bank, and wire frauds, identity theft, and related crimes, and the use of computers, cell phones, and other electronics to commit these crimes. My formal education also includes a B.A. from the University of California, Irvine, and a J.D. from the University of Southern California. I have led and participated in many aspects of criminal investigations, including: collecting and reviewing physical and electronic evidence; conducting surveillance; utilizing informants; interviewing witnesses, subjects, and targets of investigation; and preparing and serving subpoenas, search and arrest warrants, and other legal process.

6. As an HHS-OIG Special Agent, I am a federal law enforcement officer within the meaning of 5 U.S.C. § 406, in that I am empowered by law and authorized by the Attorney

General to conduct investigations, seek and execute warrants, and make arrests for federal offenses.

7. I am currently assigned to investigate complex financial crimes involving HHS-funded programs in the Central and Southern Districts of California. I am working in conjunction with the United States Secret Service ("USSS"), Homeland Security Investigations ("HSI"), and the El Camino Real Financial Crimes ("ECR") Task Force. The ECR Task Force is an HSI-sponsored task force comprised of local, state, and federal law enforcement personnel, whose duties are to investigate cyber and financial crimes, including activity in connection with the fraudulent use of access devices, payment card skimming and re-encoding, identity theft, money laundering, and other frauds.

III. SUMMARY OF PROBABLE CAUSE

8. Between January 2024 and January 1, 2025, the California Department of Social Services ("DSS") has detected more than \$126.8 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. This fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

9. On May 1, 2025, beginning at approximately 5:30 a.m., law enforcement conducted physical surveillance at a Wells Fargo Bank located at 3508 East Florence Avenue, Huntington Park, CA (the "Target Bank"), and at a laundromat located at 3046 East Florence Avenue, Huntington Park, CA (the "Target Laundromat"),

both of which were identified by DSS as among the top ATM locations for EBT fraud.

10. At approximately 6:40 a.m., law enforcement saw DINCA and COCORA arrive together in a tan Buick sedan at an ATM terminal located at the Target Bank where law enforcement was conducting surveillance. Law enforcement observed DINCA and COCORA, taking turns between sitting in their car and interacting with the ATM, withdraw approximately \$5,460 in cash from the ATM in rapid succession using approximately five different access devices. Law enforcement then followed DINCA and COCORA to the vicinity of the Target Laundromat, where DINCA was observed withdrawing approximately \$2,280 in cash from the ATM inside the laundromat in rapid succession using approximately five different access devices. Law enforcement ultimately detained DINCA and COCORA and found a total of approximately 20 access devices (later determined to be cloned cards, 12 of which had the same EBT card information DINCA and COCORA used to withdraw a total of \$7,740 in cash from ATMs at the Target Bank and Target Laundromat). DINCA was arrested and found to be in possession of bulk cash, approximately seven access devices, and the SUBJECT DEVICE. COCORA was arrested and found to be in possession of bulk cash and approximately 13 access devices.

IV. STATEMENT OF PROBABLE CAUSE

11. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

12. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

13. The U.S. Department of Health and Human Services, Administration for Children and Families, administers the Temporary Assistance to Needy Families ("TANF") program. TANF is a federally funded assistance program that awards grants to individual states to support low-income families with children. In California, TANF grant funds are used to operate CalWORKs.

14. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

15. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions.

For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

16. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

17. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

18. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

B. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations

19. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement

determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

20. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

21. On a legitimate debit or credit card, the information contained on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information contained on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be encoded with the EBT card information, but the card itself will still bear the embossed information of the gift card or bear no information if it is a blank white plastic card.

22. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested

to clone cards is often obtained from what is colloquially referred to as "skimming activity."

23. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

24. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

25. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period

of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

26. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

27. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud

ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than \$190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than \$70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

28. In or about March 2023, federal law enforcement conducted another surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed

at select high-volume EBT fraud ATMs. Law enforcement arrested eleven suspects that conducted a high volume of unauthorized transactions and that conducted those transactions in rapid succession. At the time of their arrest, the suspects had in their possession over 400 cloned cards, \$120,000 in illicitly obtained funds, and multiple skimming devices.

29. Ten out of the eleven of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States.

C. Background of Current Operation to Combat EBT Fraud

30. The most current data provided by DSS, based in part upon reported fraud by victims, indicates that between January 2024 and January 1, 2025, more than approximately \$126.8 million in cash benefits has been stolen from victim EBT cards throughout California.

31. Of the more than approximately \$126.8 million in cash benefits stolen during this year time period, more than approximately \$57.9 million has been stolen from victim EBT cards, in the county of Los Angeles alone. The majority of these funds were stolen through unauthorized ATM withdrawals.

32. Between on or about December 1, 2024, and on or about December 31, 2024, according to data from DSS, more than approximately \$11.4 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately \$11.4 million stolen from victim EBT cards in the month of December 2024, more than approximately \$6.2 million was

stolen, mostly through unauthorized ATM withdrawals, in Los Angeles County alone.

33. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

34. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

35. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all

cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

D. DINCA and COCORA Committed EBT Fraud Using Unauthorized Access Devices on May 1, 2025

36. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement conducted a surveillance and arrest operation in May 2025.

37. Based upon my training and experience, I know EBT cardholders are not able to conduct cash withdrawals from their EBT cards until approximately 6:00 a.m.

38. On or about May 1, 2025, beginning at approximately 5:30 a.m., law enforcement began surveillance on the Target Bank and the Target Laundromat.

39. At approximately 6:40 a.m., based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, DINCA and COCORA arrived at the Target Bank together in a tan Buick sedan and took turns using the ATM terminal. Law enforcement saw both DINCA and COCORA conduct multiple transactions, which appeared to be withdrawals based upon law enforcement observing DINCA and COCORA retrieve what appeared to be currency at the conclusion

of each transaction. Law enforcement saw DINCA and COCORA, for approximately three minutes each, conducting what appeared to be several withdrawal transactions in rapid succession. Law enforcement observed both DINCA and COCORA appear to insert several different cards to conduct withdrawals and store the retrieved currency on their person on several occasions. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not transition between multiple payment cards rapidly to conduct several transactions in a short period of time.

40. At approximately 6:45 a.m., DINCA and COCORA left the Target Bank together in the tan Buick sedan. Without losing sight of the car, agents followed DINCA and COCORA to the vicinity of the Target Laundromat. The Buick sedan parked across the street from the Target Laundromat. DINCA exited the car while COCORA remained inside the car. Agents saw DINCA inside the Target Laundromat conducting transactions at the ATM. DINCA was at the ATM conducting multiple withdrawal transactions in rapid succession for approximately eight minutes.

41. Based on the date, time, ATM locations, presence of multiple, and successive ATM withdrawals on multiple EBT cardholder accounts during a short time period, law enforcement detained both DINCA and COCORA in order to investigate further.

42. DINCA had a large amount of cash, approximately seven cloned cards, and the SUBJECT DEVICE in his jacket and pants pockets. Six of the cloned cards consisted of gold-colored

Vanilla Visa gift cards. The remaining cloned card was a black-colored Green Dot Visa debit card. The cards also had stickers placed on them with, what appeared to be, based on my training and experience, card balances and victim PINs. The following photo is an example of a seized cloned card:



43. COCORA was detained as she got out of the tan Buick sedan from the front passenger seat. Inside the car, agents found a large amount of cash stored in the glove compartment. In the center console, agents also found a purse that contained approximately 11 cloned cards. Two additional cloned cards were found hidden underneath the front passenger-side floor mat.

44. I analyzed the magnetic stripe of the cloned cards and determined all of them were encoded with mismatching card numbers. All 20 of the cards were encoded with EBT BINs. Moreover, the cloned cards also were affixed with stickers bearing victim PIN numbers and balances that closely corresponded to each cloned card and withdrawal amount and were needed in order to conduct the unauthorized ATM withdrawals.

45. Based on my review of law enforcement reports, conversations with other law enforcement agents, my own knowledge of the investigation, and EBT card transaction data

obtained from DSS, I know that, at the Target Bank, agents saw DINCA and COCORA conduct approximately seven transactions involving EBT card numbers -- all of which matched EBT card numbers encoded on the cloned cards seized from the car in which COCORA was arrested. I also know that, at the Target Laundromat, agents saw DINCA conduct approximately 13 transactions involving EBT card numbers -- all of which matched EBT card numbers encoded on the cloned cards seized from DINCA's person during his arrest. Nineteen of the 20 total transactions conducted between the Target Bank and Target Laundromat were successful withdrawals totaling \$7,740 in financial loss. The remaining withdrawal was an attempted but not authorized transaction totaling \$920 in attempted financial loss.

46. Based on my review of EBT cardholder information obtained from DSS, none of the EBT cards transacted by DINCA and COCORA belonged to them.

47. During arrest processing, both DINCA and COCORA stated that they were citizens and nationals of Romania. U.S. law enforcement database queries corroborated DINCA's identity and nationality based on matches in biographic information. Romanian government officials confirmed COCORA's identity based on matches in photographs and biographic information.

48. The SUBJECT DEVICE was retrieved from DINCA's pockets and secured in law enforcement custody pending issuance of a search warrant.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

49. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers or cellular telephones.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their

digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos.

Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

50. As used herein, the term "digital device" includes the SUBJECT DEVICE.

51. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

52. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

53. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

54. For all of the reasons described above, there is probable cause to believe that DINCA and COCORA have committed violations of 18 U.S.C. § 1029(a)(2), (b)(1), (c)(1)(A)(i) (use

and attempted use of unauthorized access devices).. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE as described in Attachment A.

Attested to by the applicant in
accordance with the requirements
of Fed. R. Crim. P. 4.1 by
telephone on this 2nd day of May,
2025.

A handwritten signature in blue ink, appearing to read 'M. Kaufman', is written over a horizontal line.

THE HONORABLE MICHAEL KAUFMAN
UNITED STATES MAGISTRATE JUDGE